Office of Thrift Supervision
Department of the Treasury

1700 G Street, N.W., Washington, D.C. 20552

John F. Downey
Executive Director, Supervision

October 24, 1996

MEMORANDUM FOR: Chief Executive Officers

FROM: John Downey
Executive Director, Supervision

SUBJECT: Risk Management of Client/Server Systems

Enclosed for your review is an interagency statement on risk management of client/server computer systems developed by the Federal Financial Institutions Examination Council (FFIEC). The statement encourages senior management of financial institutions to develop and implement sound policies, practices, and procedures to mitigate risks posed by a client/server environment.

Mr. Paley Pang would be pleased to answer any questions you have about this statement. He can be reached at (415) 616-1554.

Enclosure

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202) 634-6526 • FAX (202) 634-6556

RISK MANAGEMENT OF CLIENT/SERVER SYSTEMS

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior management of each FFIEC Agency, and all examining personnel.

PURPOSE

The purpose of this document is to alert the Boards of Directors and senior management of financial institutions to risks associated with client/server computing and to encourage the development and implementation of sound policies, practices, or procedures and controls over client/server computing environments.

BACKGROUND

The traditional approach to data processing for banking functions has been to develop and use large mainframe or midrange systems which are expensive to acquire and maintain. These systems require special physical environments and lengthy application development processes. Application developers have not always kept up with development requests that would allow financial institutions to provide faster delivery of services and products. End-users, who need immediate solutions, have become frustrated with this traditional approach to data processing. New technology is now available, at a perceived cost savings, that could satisfy end-user demand for more timely management information system solutions.

End-user needs have led to increasing acquisitions of computers and commercial off-the shelf programs by departments, business units, and individuals to reduce their dependence on a centralized data processing environment. However, this strategy has its own limits. For example, stand-alone computers make it difficult to share information with other information systems. This problem is being solved by the development of high-speed data transmission and network file servers in client/server computing.

As a result, financial institutions are now processing mission-critical applications including funds transfer, branch automation, general ledger reporting, security portfolio accounting, and customer relationship management on client/server systems. Additionally, independent service providers (service bureaus) are also utilizing this new technology by providing these systems as part of their servicing operations to financial institutions.

POLICY STATEMENT

It is the responsibility of the Board of Directors of financial institutions to develop and adopt appropriate policies, practices, or procedures covering management's responsibilities and controls for all areas of client/server computing activities. Management must recognize that the implementation of controls is just as important in the client/server environment as in the mainframe environment. The institution's strategic planning should clearly define the technological and control architecture. End-users and auditors must have a prominent role in the acquisition, development, and implementation of all client/server computing environments.

The existence of policies, practices, or procedures and the management supervision of client/server activities will be evaluated by examiners during regular supervisory reviews of the institution.

DEFINITION

Client/server computing is a method of allocating data processing resources in a network so that computing power is distributed among workstations in the network. This type of computing allows integrated applications (general ledger, demand deposit accounting, loans, etc.) to share system and data resources using cooperative processing. Cooperative processing differs from traditional mainframe or distributed system processing in that each processing component is mutually dependent.

CONCERNS

The proliferation of client/server technology introduces new risks as well as benefits. In today's competitive environment, client/server technology can be a strategic initiative of the organization, and therefore is not just a technological concern, it is also a business concern. Customer demand for flexible and timely management information has fostered its growth. Faster delivery of services, ability to leverage emerging technology, autonomy of end-users, and productivity gains from re-engineering the work flow are all potential benefits.

The client/server architecture has not evolved to the point where controls are inherent in the design, maintenance, and operation of the system. Controls are more difficult to implement effectively due to the distributed, decentralized and complex nature of the client/server environment. The tables that appear later in the paper illustrate some of the risks and controls that have been associated with client/server computing.

The appendix to this issuance identifies components and characteristics of client/server computing.

SECURITY

Supervisory Concerns	Controls
Adequate physical security for critical hardware components may not be present due to the distributed nature of the environment and the slow development of security conscious cultures in the client/server arena. Inadvertent or intentional unauthorized end-user access to software and data presents greater risk of loss in client/server environments due to a potential dependence on the end-user to implement some system functions.	Adequate steps should be taken to ensure protection from unauthorized access, use of, or changes to, systems or data. Procedures should be implemented to ensure the privacy and confidentiality of information.

COMPUTER OPERATION

Supervisory Concerns	Controls
Disaster recovery and business continuation plans may be incomplete or outdated due to more frequent changes to hardware and software resources. Exposure to system failures may be increased due to easier software virus infiltration in a distributed environment. Incomplete hardware and software inventories could result in additional exposures in the form of unidentified network operations and/or the lack of adequate insurance coverage. Management information systems that rely on client/server systems could become incomplete or inadequate due to the lack of adequate operational controls. The lack of or inadequate network configuration diagrams could result in ineffective management oversight.	Procedures should be adequate to ensure the timely, accurate, and complete processing of information. Management should ensure that critical systems and operations are recoverable in the event of a disruption in service.

IMPLEMENTATION AND MAINTENANCE

Supervisory Concerns	Controls
Internal control considerations could be neglected due to the shortened time frames commonly found in the development of client/server systems. System failures resulting in weaknesses not identified in pre-implementation testing are more likely to occur than in mainframe environments. There are increased risks from unauthorized modification of application programs due to the distributed location of the client and its applications. Application development costs may consistently be underestimated if a system development life cycle methodology is not used. Failure to re-engineer the work flow in the design phase of the application may limit management's ability to optimize the benefits from this technology.	Appropriate procedures including a system development life cycle methodology should be included in new and existing client/server systems.

SYSTEMS SOFTWARE

Supervisory Concerns	Controls
In this heterogenous environment (i.e., consisting of multiple platforms), there is an increased vulnerability to incompatibilities in installed software versions. Thus modifications may cause inconsistent operating results.	Management should ensure that systems are properly tested and approved and that modifications are properly implemented. Management should determine that adequate version control procedures are properly implemented.

DATABASE MANAGEMENT SOFTWARE

Supervisory Concerns	Controls
Database integrity may be corrupted by deficiencies in the quality of the implementation and the administration of database management systems. Lack of database integrity is of greater concern due to concurrent updates of distributed databases which may not have properly established locking capabilities. Unauthorized access to the data could occur as a result of inadequate database administration or improper data ownership.	Management should ensure that controls are implemented to ensure the integrity of transactions. Management should ensure that systems are properly tested and approved and that modifications are properly implemented. Management should determine that adequate version control procedures are properly implemented. Management should determine that the database management system has adequate recovery capabilities.

MIDDLEWARE

Supervisory Concerns	Controls
System integrity may be adversely effected due to multiple operating environments attempting to interact concurrently.	Management should ensure that controls are implemented to ensure the integrity of the client/server networks.
Lack of proper software change procedures across multiple platforms could result in a loss of system integrity.	Management should ensure that systems are properly tested and approved and that modifications are properly implemented. Management should determine that adequate version control procedures are properly implemented.

APPENDIX

RISK MANAGEMENT OF CLIENT/SERVER SYSTEMS

CLIENT/SERVER COMPONENTS AND CHARACTERISTICS

Components of client/server computing include:

- CLIENT — A client (front-end) is a single PC or workstation associated with software that provides computer and presentation services as an interface to server resources. Presentation is usually provided by visually enhanced processing software known as a Graphical User Interface (GUI).

- SERVER — A server (back-end) is one or more multi-user computer(s), usually a mainframe or a minicomputer, although it could be a PC. Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, facsimile services, application development, and others. Multiple functions may be supported by a single server.

- MIDDLEWARE — This is a client/server specific term used to describe a unique class of software employed by client/server applications. This software resides between an application and the network, and manages the interaction between the GUI front-end and data servers in the back-end. It facilitates the client/server connections over the network and also allows client applications to access and update remote databases and mainframe files.

Characteristics of client/server computing include:

- DISTRIBUTED — Most commonly, a server is a distinct computer that serves from a few to any number of client systems. It is feasible to have clients and servers on the same computer. The server may be in the same room as its clients, or it may be across town or around the world.

- DECENTRALIZED — Client/server systems are typically installed, administered, and operated by a business unit, rather than a centralized computing facility.

- COMPLEX — Client/server systems usually involve multiple clusters of computers linked by high-speed communication lines.